

AFFIDAVIT

I, Michael Prete, Special Agent, Federal Bureau of Investigation (“FBI”), being duly sworn, declare and state as follows:

INTRODUCTION & PURPOSE OF THE AFFIDAVIT

1. I make this affidavit in support of an application for the issuance of a seizure warrant to seize all assets stored in the Binance accounts for User Identification Number (UIN) 518226780 held in the name of ODAI AHMAD YASIN ALZAYADNEH (Odai Binance Account) and all assets stored in the Binance accounts for User Identification Number (UIN) 355360441 held in the name of SALEEM EMAD SALEEM AHMAD (Saleem Binance Account) (collectively **Target Assets**).

2. The Target Assets are believed to constitute or be derived from proceeds traceable to Wire Fraud (18 U.S.C. § 1341) and property involved in Concealment Money Laundering (18 U.S.C. § 1956(a)(1)(B)(i)). For the court to authorize seizure of the Target Assets, it must find probable cause to believe that: (1) the crimes of Wire Fraud and/or Concealment Money Laundering were committed; and (2) the Target Assets have a connection to those offenses in the manner specified by the below statutes authorizing forfeiture.

3. For the reasons set forth below, there is probable cause to believe the Target Assets have a connection to Wire Fraud and Concealment Money Laundering and are subject to **civil seizure and forfeiture** under the following forfeiture authorities:

- a. Pursuant to 18 U.S.C. § 981(a)(1)(C) because the Target Assets are property, real or personal, which constitutes or are derived from proceeds traceable to a Wire Fraud. Section 981(a)(1)(C) provides for the civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds from any offense

constituting a “specified unlawful activity” as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offenses. A “specified unlawful activity,” as defined in Section 1956(c)(7), includes offenses listed in 18 U.S.C. § 1961(1). Section 1961(1) includes Wire Fraud violations.

- b. Pursuant to 18 U.S.C. § 981(a)(1)(A) because the Target Assets were involved in Concealment Money Laundering or are traceable to such property.
- c. Consequently, seizure of the Target Assets for civil forfeiture is authorized by 18 U.S.C. § 981(b).

4. For the reasons set forth below, there is probable cause to believe the Target Assets have a connection to Wire Fraud and Concealment Money Laundering and are subject to **criminal seizure and forfeiture** under the following forfeiture authorities:

- a. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c) because the Target Assets are property, real or personal, which constitutes or are derived from proceeds traceable to Wire Fraud.
- b. Pursuant to 18 U.S.C. § 982(a)(1) because the Target Assets were involved in Concealment Money Laundering or is traceable to such property.
- c. Consequently, seizure of the Target Assets for criminal forfeiture is authorized by 21 U.S.C. § 853(f) and 18 U.S.C. § 982(b).

5. With respect to seizure for criminal forfeiture, 21 U.S.C. § 853(f) provides that a court may issue a criminal seizure warrant when it “determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a protective order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture.” There is a substantial risk that the assets discussed in this affidavit will

be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless immediate steps are taken to secure them through a seizure warrant. As all forms of cryptocurrency, the assets discussed in this affidavit are inherently portable and fungible. Furthermore, many cryptocurrencies are subject to speculative valuations and volatile price swings. Even a so-called “stablecoin” cryptocurrencies pegged to fiat currency (such as Tether, which is tied to the U.S. dollar) faces substantial questions about the assets backing the cryptocurrency and whether the cryptocurrency would withstand, for example, a run on the cryptocurrency caused by a drop in investor confidence. Thus, even assuming the targets of this investigation could be located and extradited for prosecution, there is a substantial possibility that the assets discussed in this affidavit would experience a significant devaluation before any orders of forfeiture could be imposed pursuant to conviction of the targets. I therefore submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the assets will remain available for forfeiture and ask the Court to so find in authorizing the seizure warrant.

6. Although Rule 41(b) of the Federal Rules of Criminal Procedure provides that seizure warrants must be executed in the issuing district, other statutes authorize a magistrate to issue a warrant to seize property outside the district. Under 21 U.S.C. § 853(l), district courts have jurisdiction to authorize a criminal seizure warrant under 21 U.S.C. 853(f) “without regard to the location of any property which may be subject to forfeiture.” Similar authority is granted by 18 U.S.C. § 981(b)(3) for civil forfeiture seizure warrants under 18 U.S.C. § 981(a). Binance is in the Seychelles, but it accepts U.S. warrants.

BACKGROUND OF AFFIANT

7. I am a Special Agent with the FBI in Salt Lake City, Utah. I have been an FBI Special Agent since February 12, 2023. In my capacity as a Special Agent with the FBI, I have

conducted and participated in numerous official investigations into wire fraud, money laundering and other financial and computer crimes. I am a graduate of the FBI Training Academy in Quantico, Virginia and have also attended advanced training classes in the areas of cybercrime.

8. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

BACKGROUND ON CRYPTOCURRENCY

9. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat (i.e. national currencies like the dollar, euro, yen, etc.) currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most

cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.¹ Cryptocurrency is not illegal in the United States.

b. Bitcoin² (“BTC”) is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it’s not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

c. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a

¹ Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

² Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key”). A public address is represented as a case-sensitive string of letters and numbers, 26–35 characters long. Each public address is controlled and/or accessed using a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’ private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

d. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services on hidden services websites. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track transfers, trades, purchases, and other financial transactions. As of March 28, 2022, one bitcoin is worth approximately \$47,741 though the value of bitcoin is generally much more volatile than that of fiat currencies.

e. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet (“mobile wallet”), printed public and private keys (“paper wallet”), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code³ with the public and private key embedded in the code. Paper wallet keys are not

³ A QR code is a matrix barcode that is a machine-readable optical label.

stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured if their assets become potentially vulnerable to seizure and/or unauthorized transfer.

f. Bitcoin “exchangers” and “exchanges” are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.⁴ Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures like those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers’ desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

⁴ See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

g. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

RELEVANT CRIMINAL STATUTES

10. Title 18 U.S.C. § 1343 states:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio or television communication in interstate or foreign commerce, any writings, signs, signals, pictures . . . for the purpose of executing such scheme or artifice.

11. Title 18 U.S.C. § 1956(a)(1)(B)(i) states:

Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(B) knowing that the transaction is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

FACTS

12. This case involves the receipt of funds into the Target Assets consisting of proceeds from a cryptocurrency technical support scam. My investigation has revealed that the Target Assets is financed by the transfer of fraudulent proceeds received from victims of technical support schemes.

13. The Victim 1 held cryptocurrency in a Coinbase account. The Victim 1 received a phone call from an Unknown Subject (“Unsub 1”). Unsub1 told the Victim 1 that Coinbase had been compromised, and that the Victim 1 would need to transfer his Coinbase assets from the Coinbase exchange to a Coinbase wallet. Unsub 1 directed the Victim to set-up a wallet. Unsub 1 directed the Victim 1 to transfer three of the Victim 1’s largest cryptocurrency assets, which the Victim 1 did. After the transfer, the Victim 1 realized that the cryptocurrency had been moved out of his newly created wallet. Victim 1 did not initiate these transfers. Victim 1 did not knowingly provide any passwords or seed phrases to Unsub 1 and is not sure how the bitcoin was moved out of his new wallet.

14. Victim 1’s bitcoin was sent through a series of cold wallets,⁵ swapped out for USDT,⁶ before arriving in two Binance Wallets. Exhibits 1 and 2 depict the tracing of the Victim 1’s bitcoin into a wallet within the Odai Binance Account. Exhibits 3 and 4 depict the tracing of the Victim 1’s bitcoin into a wallet within the Saleem Binance Account.

15. In tracing funds, investigators used a last in first out methodology. This method assumes that when dirty funds (last in) are deposited into an account/wallet then those dirty funds must be spent first (first out) even when subsequent “clean” funds are deposited. Once the entirety

⁵ A cold wallet is a wallet for holding cryptocurrency that is not associated with a specific cryptocurrency exchange.

⁶ USDT is a type of cryptocurrency on the Ethereum blockchain tied to the value of the US dollar.

of the dirty funds are spent, then the clean funds are used for withdrawals. Courts have recognized the use of tracing methods to trace criminal proceeds including in *United States v. Banco Cafetero Panama*, 797 F.2d 1154 (2d Cir. 1986) (approving the use of accounting methods to trace criminal proceeds; government can choose the method).

16. The following is a summary of the movement of funds from the Victim 1's wallet to a wallet within the Odai Binance Account, which corresponds to the charts in Exhibit 1 and 2:

- a. On 12/02/2024 at 11:15 PM bc1qneaplhs2tl4akuwclnr6ra46g38mm3qedp9gk8 (Victim 1's Wallet) sent 1.5695 BTC to bc1qngfyp38hclzv4n9jkw7hjvlpmmq20ew2el (Cold Wallet 1).
- b. On 12/03/2024 at 01:14 AM bc1qngfyp38hclzv4n9jkw7hjvlpmmq20ew2el (Cold Wallet 1) sent 1.617 BTC to bc1qsstgtaler6rq6tsze68fdty56mhspdhwxguuw (Cold Wallet 2).
- c. On 12/03/2024 at 01:39 AM bc1qsstgtaler6rq6tsze68fdty56mhspdhwxguuw (Cold Wallet 2) sent 1.617 BTC to bc1q8vvyqtvz8td52aj56kqm4xpac885gyut8ymjr7 (Cold Wallet 3).
- d. On 12/03/2024 at 04:25 AM bc1q8vvyqtvz8td52aj56kqm4xpac885gyut8ymjr7 (Cold Wallet 3) sent 1.0965 BTC to bc1qw8fea80cn3mxw9mcgmqevax2elz7tpsylajpl8 (Cold Wallet 4).
- e. On 12/05/2024 at 12:13 PM bc1qw8fea80cn3mxw9mcgmqevax2elz7tpsylajpl8 (Cold Wallet 4) sent 1.0965 BTC to 12KiYhb8trvKQSS6CpMNgjTbKBSi35FwPz (Cold Wallet 5).

- f. On 12/05/2024 at 01:38 PM 12KiYhb8trvKQSS6CpMNgjTbKBSi35FwPz (Cold Wallet 5) sent 1.0965 BTC to bc1qena5rwnjy603gyz5cwhl0zelhyxqtuad98jd5q (Thor Swap).
- g. On 12/05/2024 at 03:11 PM 0xd37bbe5744d730a1d98d8dc97c42f0ca46ad7146 (Thor Swap) sent 112018.6265 USDT to 0xc89d2117a01205b9e301143d60add056da4c083 (Thor Swap Recipient Wallet).
- h. On 12/05/2024 at 03:17 PM 0xc89d2117a01205b9e301143d60add056da4c083 (Thor Swap Recipient Wallet) sent 113888 usdt to 0x5f25f7b99a5603f0994ceb962eeeb7d99bcc0e1d (Cold Wallet 6).
On 12/19/2024 at 01:22 PM 0x5f25f7b99a5603f0994ceb962eeeb7d99bcc0e1d (Cold Wallet 6) sent 100000 USDT to 0x8bf925c7a6feba275618f8f2a089198458c0ad15 (wallet within the Odai Binance Account).

17. The following is a summary of the movement of funds from the Victim 1's wallet to a wallet within the Saleem Binance Account, which corresponds to the charts in Exhibit 3 and 4:

- a. On 12/02/2024 at 11:15 PM bc1qneaplhs2tl4akuwclnr6ra46g38mm3qedp9gk8 (Victim 1's Wallet) sent 1.5686 btc to bc1qngfyp38hclzv4n9jkw7hjavlwpmmyq20ew2el
- b. On 12/03/2024 at 01:14 AM bc1qngfyp38hclzv4n9jkw7hjavlwpmmyq20ew2el sent 1.617 btc to bc1qsstgtaler6rq6tsze68fdty56mhspdhwxguquw

- c. On 12/03/2024 at 01:39 AM bc1qsstgtaler6rq6tsze68fdty56mhspdhwxguquw sent 1.617 btc to bc1q8vvyqtvz8td52aj56kqm4xpac885gyut8ymjr7
- d. On 12/03/2024 at 04:25 AM bc1q8vvyqtvz8td52aj56kqm4xpac885gyut8ymjr7 sent 0.5205 btc to 3FcWHCMbsTekN5KsvyJbQoWAGLv2RaT6A9 (OKX Inflow)
- e. On 12/03/2024 at 04:50 AM 0x06959153b974d0d5fd87d561db6d8d4fa0bb0b (OKX Outflow) sent 50000 usdt to 0x30b153b77ba6d6b8660cbd35b57739f2dd49fa0a
- f. On 12/03/2024 at 01:44 PM 0x30b153b77ba6d6b8660cbd35b57739f2dd49fa0a sent 39265 usdt to 0x1dbfc03cee195c82c305e8ad63b3b4f1bb0db2a8 (wallet within the Saleem Binance Account).

18. On January 9, 2025, Detective Miranda Smidt (“SMIDT”), from Financial Crimes Investigations of the Colorado Springs Police Department, also requested a freeze on account 0x8bf925c7a6feba275618f8f2a089198458c0ad15, the same wallet within the Odai Binance Account the Victim 1’s funds were traced to. SMIDT requested that Binance freeze the account after determining that the account had received victim funds. The transaction containing the victim funds was from November 11, 2024. SMIDT determined that \$13,825.974341 USDT in funds were attributed to account 0x8bf925c7a6feba275618f8f2a089198458c0ad15. The victim in SMIDT’s investigation (“Victim 2”), was contacted by an unknown individual (“Unsub 2”). Unsub 2 claimed to be from “Coinbase Security”. Unsub 2 told Victim 2 that Victim 2’s Coinbase account was compromised. Unsub 2 guided Victim 2 to send all of Victim 2’s funds to a new “Coinbase” wallet. In total, Victim 2 lost approximately \$100,125.

19. Upon the issuance of a freeze request for Odai Binance Account, the owner of the Odai Binance Account contacted the FBI. The SUBJECT, located in the Hashemite Kingdom of Jordan, claimed that the Odai Binance Account was used for his business. According to the SUBJECT, the SUBJECT would exchange cryptocurrency for physical currency, at the request of customers. The SUBJECT provided business documentation in support of the SUBJECT's claims. The provided documentation was from The Hashemite Kingdom of Jordan, Jerash Chamber of Commerce. However, the provided documentation was for an electronic marketing business, as opposed to a currency exchange service. Furthermore, the provided documentation only allowed the SUBJECT to operate the SUBJECT's business within 2023. The SUBJECT also provided a link to a Facebook page, which the SUBJECT claimed was his official business page. Investigation into the SUBJECT's claims is ongoing.

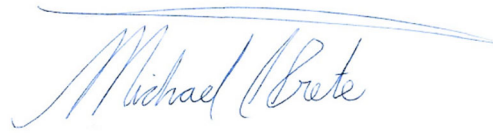
20. The Target Assets are subject to forfeiture and seizure as either proceeds of wire fraud and/or property involved in concealment money laundering. This includes assets in the Target Assets that are not proceeds of or traceable to proceeds of the fraud because the non-traceable assets were involved in money laundering. "When money from illegal sources is commingled with money from unspecified other sources, 'all such funds are attributable to the money laundering scheme.'" *United States v. Jamieson*, 427 F.3d 394, 404 (6th Cir. 2005) (quoting *United States v. Owens*, 159 F.3d 221, 229 (6th Cir.1998)). Assets "involved in the offense," including entire accounts where only a portion of the incoming funds were traceable to fraud, are forfeitable. *United States v. Certain Funds on Deposit in Account No. 01-0-71417*, 769 F. Supp. 80, 84 (E.D.N.Y. 1991) (explaining that 18 U.S.C. § 981(a)(1)(A) "has been construed by the district courts as authorizing the forfeiture of an entire bank account or business which was used to 'facilitate' the laundering of money in violation of 18 U.S.C. § 1956 . . . [e]ven if a portion of the

property sought to be forfeited is used to ‘facilitate’ the alleged offense”) (internal citations omitted). *See also United States v. Omid*, 2021 WL 7629897 (Slip Copy) (C.D. Calif. 2021) (stating that commingling of untainted funds “with the tainted funds throughout the laundering process rendered them subject to seizure and forfeiture”). Non-tainted funds in the Target Assets facilitated the money laundering by concealing or disguising the nature, the location, the source, the ownership, or control of the fraudulently obtained proceeds.

CONCLUSION

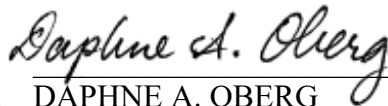
21. Based on the above and Exhibits 1, 2, 3, and 4, there is probable cause to believe that the crimes of Wire Fraud and Concealment Money Laundering have occurred and that the Target Assets are either proceeds of wire fraud and/or property involved in money laundering. Accordingly, the Target Assets are subject to forfeiture under the authorities described above.

I swear, under penalty of perjury, that the foregoing is true and correct.

A handwritten signature in blue ink that reads "Michael Prete". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Michael Prete
Special Agent - FBI

Subscribed and sworn to before me
telephonically this 15th day of January 2025.

A handwritten signature in black ink that reads "Daphne A. Oberg". The signature is cursive and elegant, with a horizontal line extending to the right.

DAPHNE A. OBERG
United States Magistrate Judge

Exhibit 1

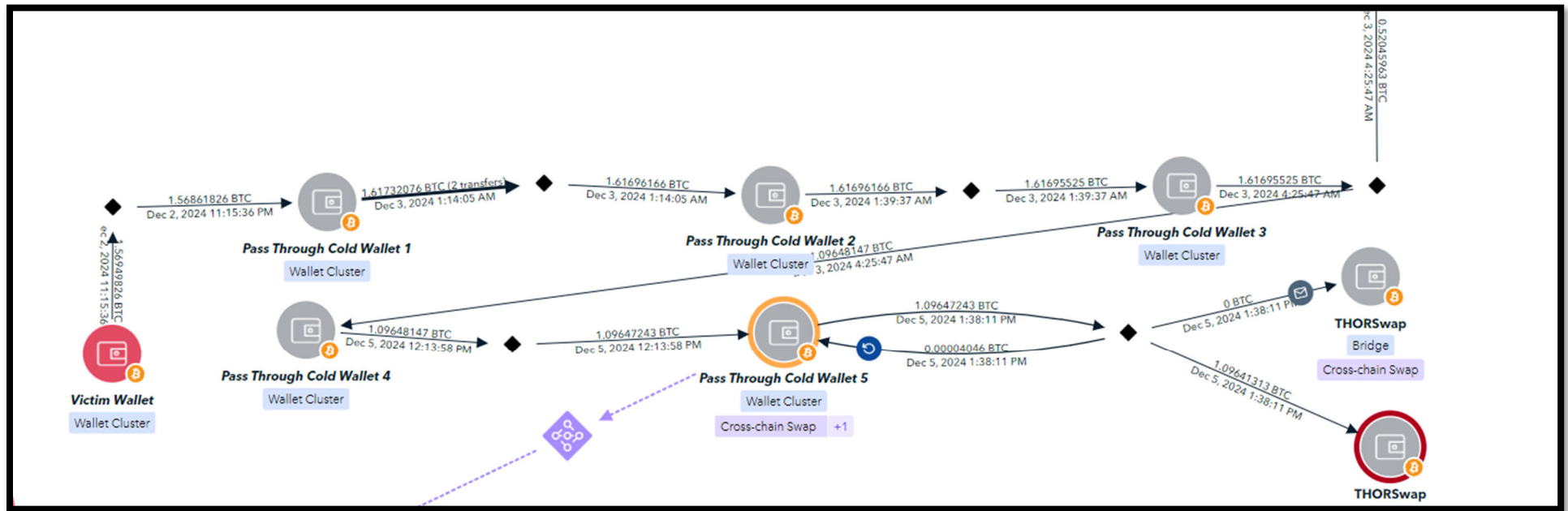


Exhibit 2

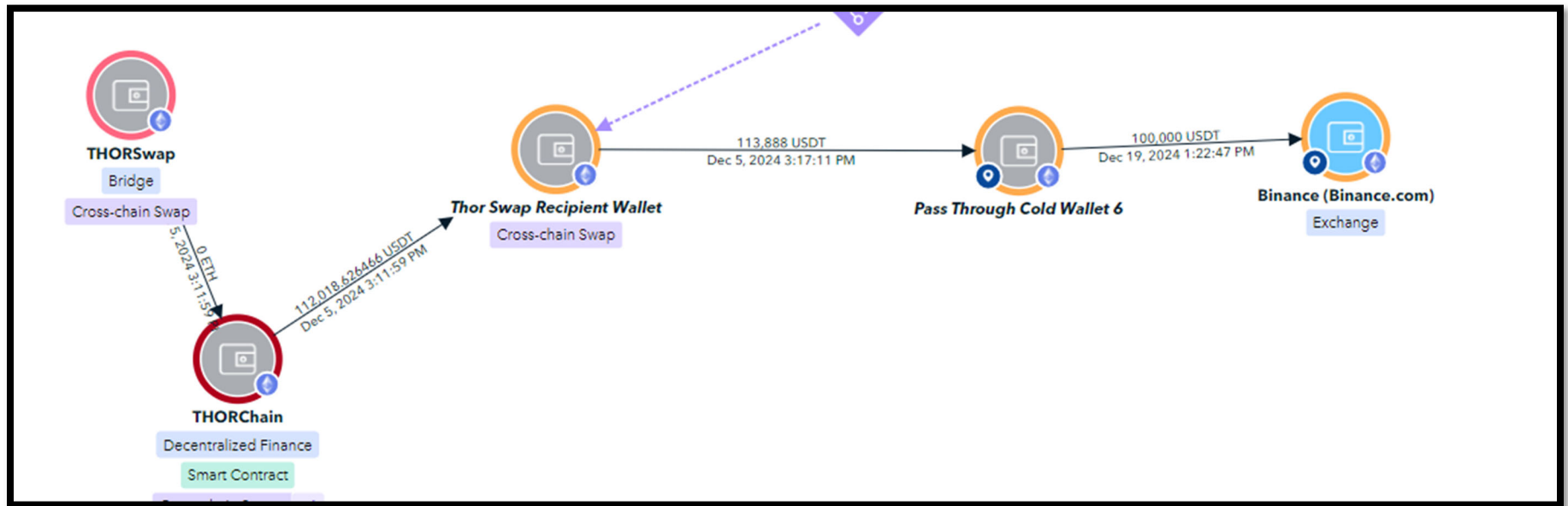


Exhibit 3

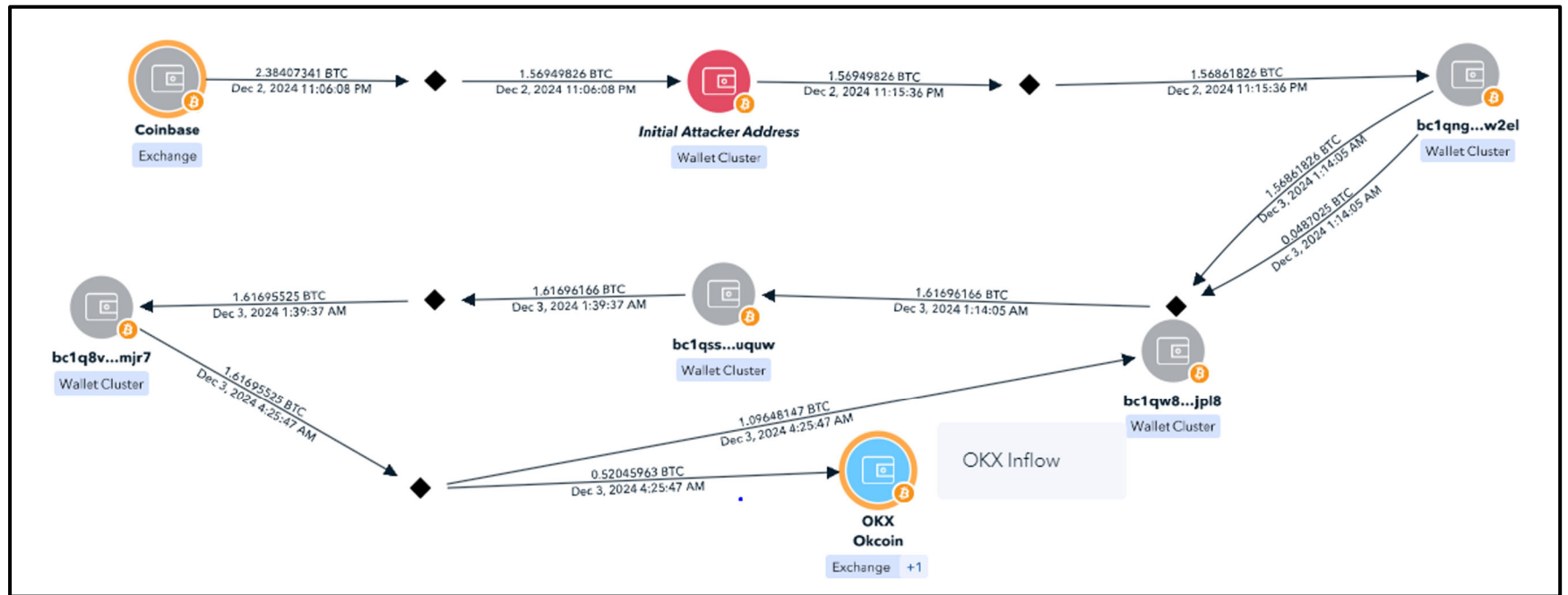


Exhibit 4

